Cum schimbi IP-ul dinamic de la Digi după o tentativă de fraudă la camerele de supraveghere (DVR)

Dacă ai un sistem de camere de supraveghere (DVR) conectat la internet, ești expus riscurilor de securitate cibernetică. Recent, m-am confruntat cu o situație neplăcută: cineva mi-a accesat ilegal serverul DVR-ului prin intermediul adresei IP.

Iată cum am rezolvat problema cu ajutorul suportului tehnic Digi și care sunt pașii exacți pe care trebuie să îi urmezi dacă treci prin aceeași situație.

Problema: Securitatea compromisă a DVR-ului

Atacatorii cibernetici scanează constant internetul după adrese IP care au porturi deschise și sisteme DVR vulnerabile (adesea lăsate cu parolele din fabrică). Odată ce îți află IP-ul și sparg parola, aceștia pot vizualiza camerele sau pot folosi echipamentul tău pentru alte atacuri.

Cea mai rapidă metodă de a le tăia accesul este **schimbarea adresei IP publice**, astfel încât atacatorii să piardă conexiunea cu rețeaua ta.

Soluția pas cu pas: Cum schimbi IP-ul dinamic la Digi

Deoarece majoritatea abonamentelor rezidențiale Digi (RCS-RDS) vin cu **IP dinamic**, adresa ta de internet se poate schimba. Suportul tehnic Digi mi-a oferit următoarea procedură simplă:

Pasul 1: Resetarea routerului/modemului

- Scoate modemul sau routerul Digi din priză.
- Așteaptă **minimum 2 minute** (acest timp este necesar pentru ca serverul Digi să elibereze IP-ul vechi alocat conexiunii tale).
- Introdu modemul înapoi în priză și așteaptă să se aprindă toate ledurile de rețea.

Pasul 2: Blocajul temporar (Ce faci dacă nu ai internet?)

După ce am reconectat routerul, am observat că laptopul meu nu avea internet nici după 10 minute. Aceasta este o problemă comună de configurare (laptopul încă încerca să folosească vechile setări de rețea).

- **Rezolvarea:** Am dat **restart la laptop**.
- Repornirea sistemului de operare forțează placa de rețea să ceară o configurație nouă (un nou IP local și noile rute DNS) de la router. După restart, internetul a funcționat perfect.

Pasul 3: Verificarea succesului

Pentru a fi sigur că atacatorii au pierdut urmărirea, am intrat pe site-ul WhatIsMyIPAddress.com înainte și după procedură. Adresa IP publică fusese schimbată cu succes!

Sfaturi cruciale pentru a preveni o nouă fraudă

Schimbarea IP-ului este doar o soluție temporară dacă nu repari vulnerabilitatea inițială. Dacă hackerii îți scanează din nou rețeaua, vor găsi noul IP. Fă imediat aceste modificări:

- **Schimbă parola DVR-ului:** Nu lăsa niciodată parole de tipul „1234”, „admin” sau „0000”. Pune o parolă complexă.
- **Schimbă porturile default:** DVR-urile folosesc porturi standard (ex. 80, 8000, 37777). Schimbă-le din setările DVR-ului și din router cu numere aleatorii (ex. 54321).
- **Dezactivează UPnP:** Oprește funcția UPnP (Universal Plug and Play) din router și din DVR, deoarece aceasta deschide porturi automat fără știrea ta.
- **Actualizează firmware-ul:** Intră pe site-ul producătorului camerelor și descarcă ultima versiune de software pentru a închide breșele de securitate.